

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-143707

(43) 公開日 平成11年(1999) 5月28日

(51) Int.Cl.<sup>9</sup>  
G 0 6 F 9/06  
A 6 1 B 5/117  
G 0 6 F 15/00  
17/60

識別記号  
5 5 0  
3 3 0

F I  
G 0 6 F 9/06  
15/00  
A 6 1 B 5/10  
G 0 6 F 15/21  
5 5 0 G  
3 3 0 F  
3 2 0  
3 4 0 B

審査請求 有 請求項の数15 O L (全 21 頁)

(21) 出願番号 特願平9-310417

(22) 出願日 平成9年(1997)11月12日

(71) 出願人 594057314

翼システム株式会社

東京都江東区亀戸2丁目25番14号

(72) 発明者 鶴村 亨三

東京都江東区亀戸2丁目25番14号 翼システム株式会社内

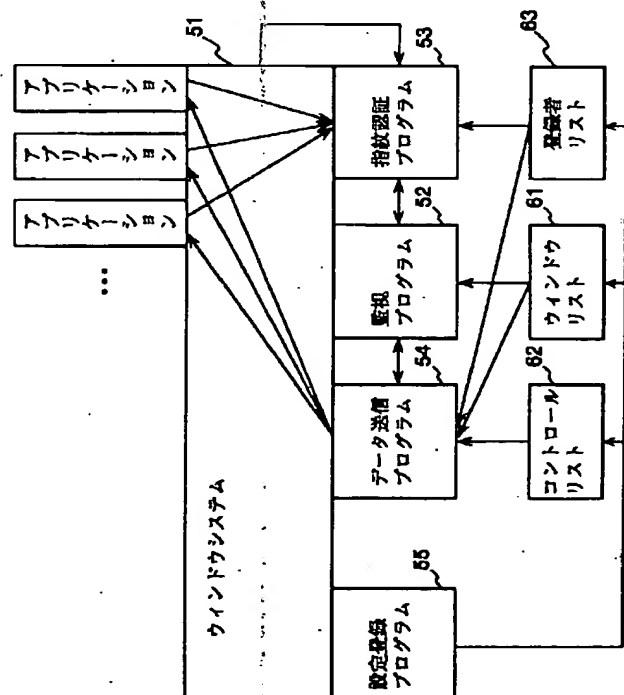
(74) 代理人 弁理士 木村 満 (外3名)

(54) 【発明の名称】 認証システム及び記録媒体

(57) 【要約】

【課題】 既存のアプリケーションを変更することなく、特定の処理の実行の可否を登録者の身体情報に基づいて決定することができる認証システム等を提供することである。

【解決手段】 ウィンドウシステム51の制御の下で動作するアプリケーションの指示により、認証対象のウィンドウが表示されたとき、監視プログラム52は、当該ウィンドウの表示を検知し、当該ウィンドウを隠すウィンドウを表示して、当該ウィンドウ上へのデータの書き込みを阻止する。次いで、指紋認証プログラム53は、指紋読取部より供給された操作者の指の輪郭の画像と、登録者リスト63に記録された、登録者の特徴データとに基づいて、当該操作者が当該登録者であるか否かを判別する。そして、当該操作者が当該登録者であると判別されると、データ送信プログラム54が、データの書き込みを阻止されたウィンドウに当該登録者が書き込むべきデータを、当該ウィンドウに書き込む。



## 【特許請求の範囲】

【請求項1】識別情報の入力要求する認証要求ウィンドウを表示し、前記識別情報が入力されたとき、所定のプログラムを実行するコンピュータ用の認証システムであって、

登録者の身体の特徴を表す身体情報と、前記識別情報とを互いに対応付けて記憶する登録者データベースと、前記コンピュータが前記認証要求ウィンドウを表示する処理を実行中であることを検出し、該認証要求ウィンドウへの前記識別情報の書き込みを阻止するウィンドウ検出手段と、

操作者の身体の特徴を表す身体情報を入力して、入力された前記身体情報と、前記登録者データベースに記憶された前記身体情報とが実質的に一致するか否かを判別する身体情報認証手段と、

前記身体情報認証手段により一致すると判別された場合に、一致すると判別された前記身体情報に対応付けられている前記識別情報を前記コンピュータに入力するデータ書込手段とを備える、

ことを特徴とする認証システム。

【請求項2】コンピュータが所定の処理に従って表示する、データの書き込みが可能なウィンドウへ、前記データを書き込むことを許すか否かを決定する認証システムであって、

前記ウィンドウを識別するウィンドウ識別情報を記憶するウィンドウ識別情報記憶手段と、

登録者の身体の特徴を表す身体情報と、前記ウィンドウに書き込むべきデータとを互いに対応付けて記憶する登録者情報記憶手段と、

前記コンピュータが、前記ウィンドウ情報識別手段に記憶されている前記ウィンドウ識別情報が示す前記ウィンドウを表示する処理を実行していることを検出し、検出された前記ウィンドウへのデータの書き込みを阻止するウィンドウ検出手段と、

操作者の身体の特徴を表す情報を入力して、入力された前記情報と、前記登録者情報記憶手段に記憶されている前記身体情報とが実質的に一致するか否かを判別する身体情報認証手段と、

一致すると判別された場合に、一致すると判別された前記身体情報に対応付けられている前記データを、前記ウィンドウ検出手段により検出された前記ウィンドウに書き込むデータ書込手段とを備える、

ことを特徴とする認証システム。

【請求項3】前記コンピュータは、識別データの書き込みを要求する認証ウィンドウを表示し、当該認証ウィンドウに書き込まれたデータが前記識別データであると判別されたとき、所定の処理を実行する識別データ認証処理を実行するものであり、

前記認証ウィンドウに書き込まれたデータが、前記識別データ認証処理に従って前記識別データであると判別さ

れるために前記データが備えるべき条件を、実質的に無作為に変更する識別データ条件変更手段と、

前記登録者情報記憶手段に記録されている、前記認証ウィンドウに書き込むべき前記データを、前記識別データ条件変更手段が変更した前記条件に合致するように変更するデータ書換手段とを備える、

ことを特徴とする請求項2に記載の認証システム。

【請求項4】前記登録者情報記憶手段は、複数の前記登録者を示す前記身体情報と、前記登録者の各々がデータを書き込むことを許される前記ウィンドウを示す前記ウィンドウ識別情報と、そのウィンドウに書き込むべきデータとを、互いに対応付けて記憶する手段を備え、

前記データ書込手段は、前記身体情報認証手段の判別結果と、前記登録者情報記憶手段に記憶されている情報とに基づき、前記ウィンドウ検出手段により検出された前記ウィンドウが、前記操作者が前記データを書き込むことを許されているウィンドウであるか否かを判別し、書き込むことを許されているウィンドウであると判別されたとき、前記操作者が当該ウィンドウに書き込むべきデータを当該ウィンドウに書き込む手段を備える、

ことを特徴とする請求項2又は3に記載の認証システム。

【請求項5】前記ウィンドウ識別情報記憶手段は、前記ウィンドウに書き込むべき前記データの種別を示す情報を、前記ウィンドウ識別情報と対応付けて記憶する手段を備え、

前記データ書込手段は、前記ウィンドウ検出手段により検出された前記ウィンドウに、前記操作者が当該ウィンドウに書き込むべき前記データのうち、当該ウィンドウに書き込むべき前記データの種別に合致すると判別されるデータを書き込む手段を備える、

ことを特徴とする請求項2、3又は4に記載の認証システム。

【請求項6】前記ウィンドウ識別情報記憶手段は、前記ウィンドウ上にある前記データの書き込み箇所を示す情報と、当該書き込み箇所に書き込むべき前記データの種別を示す情報とを、前記ウィンドウ識別情報と対応付けて記憶する手段を備え、

前記データ書込手段は、前記ウィンドウ検出手段により検出された前記ウィンドウ上にある前記データの書き込み箇所に、前記操作者が当該ウィンドウに書き込むべき前記データのうち、当該書き込み箇所に書き込むべき前記データの種別に合致すると判別されるデータを書き込む手段を備える、

ことを特徴とする請求項2乃至5のいずれか1項に記載の認証システム。

【請求項7】前記ウィンドウ識別情報記憶手段及び前記登録者情報記憶手段の少なくとも一方に格納されている情報は暗号化されており、

前記ウィンドウ検出手段及び前記データ書込手段の少な

くとも一方は、前記ウィンドウ識別情報記憶手段及び前記登録者情報記憶手段の少なくとも一方に格納されている暗号化された情報を復号化する手段を備える、ことを特徴とする請求項2乃至6のいずれか1項に記載の認証システム。

【請求項8】現在時刻を示す情報を前記身体情報認証手段に供給するタイマを備え、前記身体情報認証手段は、自らが行った前記判別の結果を示す情報及び該判別を行った時刻を示す情報を互いに対応付けて記憶するログ記録手段を備える、

ことを特徴とする請求項2乃至7のいずれか1項に記載の認証システム。

【請求項9】前記データ書込手段は、前記操作者の身体の特徴を表す情報が、前記登録者の身体の特徴を表す前記身体情報と一致しないと判別されたとき、前記ウィンドウ検出手段が検出した前記ウィンドウを消去する手段を備える、

ことを特徴とする請求項2乃至8のいずれか1項に記載の認証システム。

【請求項10】前記ウィンドウ検出手段は、前記ウィンドウ識別情報が示す前記ウィンドウが表示されたか否かを所定の時間間隔で検出する手段を備える、

ことを特徴とする請求項2乃至9のいずれか1項に記載の認証システム。

【請求項11】前記ウィンドウ検出手段は、前記ウィンドウを書き込み可能な状態で表示することを前記コンピュータに要求する命令を取得することにより、前記コンピュータが該ウィンドウを書込可能な状態で表示することを検出する手段を備える、

ことを特徴とする請求項2乃至9のいずれか1項に記載の認証システム。

【請求項12】前記登録者の身体の特徴を表す前記身体情報は、該登録者の指の特徴を示す情報からなり、前記身体情報認証手段は、前記操作者の指の特徴を示す情報を読み取る手段を備える、

ことを特徴とする請求項1乃至11のいずれか1項に記載の認証システム。

【請求項13】前記ウィンドウ検出手段は、検出した前記ウィンドウの少なくとも一部を隠蔽する手段を備える、

ことを特徴とする請求項1乃至12のいずれか1項に記載の認証システム。

【請求項14】データを入力するデータ入力処理を実行するシステムへの前記データの入力の可否を決定する認証システムであって、

前記システムが、所定の条件に合致する前記データ入力処理を実行していることを検出したとき、前記操作者による前記システムへの前記データの入力を阻止するデータ入力処理検出手段と、

前記データ入力処理検出手段により検出されるべき前記

データ入力処理を実行中の前記システムへの前記データの入力を許される者を識別する識別情報を記憶する識別情報記憶手段と、

前記操作者を特定する情報を外部より入力し、その情報と、前記識別情報とに基づき、前記操作者が、前記データ入力処理検出手段により前記データの書き込みを阻止された前記システムへの当該データの入力を許されている者であるか否かを判別し、許されていると判別されたとき、当該システムに当該データを入力するデータ入力手段とを備える、

ことを特徴とする認証システム。

【請求項15】プログラムを実行する制御部と、前記制御部が供給する命令に回答してデータの書き込みが可能なウィンドウを表示する表示部とを備えるプログラム実行手段を備えるコンピュータを、

前記ウィンドウを識別するウィンドウ識別情報を記憶するウィンドウ識別情報記憶手段と、

登録者の身体の特徴を表す身体情報と、前記ウィンドウに書き込むべきデータとを互いに対応付けて記憶する登録者情報記憶手段と、

前記プログラム実行手段が、前記ウィンドウ識別情報記憶手段に記憶されている前記ウィンドウ識別情報が示す前記ウィンドウを表示する処理を実行していることを検出し、検出された前記ウィンドウへのデータの書き込みを阻止するウィンドウ検出手段と、

操作者の身体の特徴を表す情報を入力して、入力された前記情報と、前記登録者情報記憶手段に記憶されている前記身体情報とが実質的に一致するか否かを判別する身体情報認証手段と、

一致すると判別された場合に、一致すると判別された前記身体情報に対応付けられている前記データを、前記ウィンドウ検出手段により検出された前記ウィンドウに書き込むデータ書込手段と、

して機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、認証システムに関し、特に個人情報を識別してソフトウェアの使用の可否を決定する認証システムに関する。

【0002】

【従来の技術】コンピュータシステム上で動作するアプリケーションの特定の処理の実行が、予め許可を受けた登録者以外の者により指示されないようにするための手法として、従来より、特定の画面を表示したときなどにパスワードの入力を受け付け、入力されたパスワードに基づいて登録者を認証する手法がとられている。

【0003】

【発明が解決しようとする課題】しかし、パスワードを入力する手法による場合、登録者には、パスワードを記

10

20

30

40

50

憶するという負担が課される。従って、登録者がパスワードを忘れた場合には、コンピュータシステムの管理者よりパスワードの再発行を受ける等の煩雑な手続によらなければ、パスワードの入力を条件として行われる処理が実行されない。

【0004】このような負担を解消する手法として、コンピュータが登録者の指紋などを表す身体情報を読み込んで、その身体情報により登録者を認証する手法が考えられる。ただし、この手法による場合、パスワードに基づいて認証を行う従来のアプリケーションをそのまま用いることはできない。そして、パスワードに基づいて認証を行うアプリケーションを流用するためには、アプリケーションのプログラムコードの書き換えという、煩雑で、また技術的にも困難な処理が必要となる。

【0005】この発明は上記実状に鑑みてなされたもので、既存のアプリケーションを変更することなく、特定の処理の実行の可否を登録者の身体情報に基づいて決定することができる認証システムを提供することを目的とする。

【0006】

【課題を解決するための手段】上記目的を達成するため、この発明の第1の観点にかかる認証システムは、識別情報の入力并要求する認証要求ウィンドウを表示し、前記識別情報が入力されたときと判別されたとき、所定のプログラムを実行するコンピュータ用の認証システムであって、登録者の身体の特徴を表す身体情報と、前記識別情報とを互いに対応付けて記憶する登録者データベースと、前記コンピュータが前記認証要求ウィンドウを表示する処理を実行中であることを検出し、該認証要求ウィンドウへの前記識別情報の書き込みを阻止するウィンドウ検出手段と、操作者の身体の特徴を表す身体情報を入力して、入力された前記身体情報と、前記登録者データベースに記憶された前記身体情報とが実質的に一致するか否かを判別する身体情報認証手段と、前記身体情報認証手段により一致すると判別された場合に、一致すると判別された前記身体情報に対応付けられている前記識別情報を前記コンピュータに入力するデータ書込手段とを備える、ことを特徴とする。

【0007】このような認証システムによれば、前記ウィンドウ検出手段により検出された前記認証要求ウィンドウへの前記操作者によるデータの書き込みが阻止される。そして、前記識別情報は、当該操作者が前記身体情報を提供した結果、その身体情報が前記登録者を示す前記身体情報と実質的に一致すると判別されたときに、前記データ書込手段によりその認証要求ウィンドウに書き込まれる。このため、前記所定のプログラムの実行の可否が、前記操作者及び前記登録者の身体の特徴を表す情報に基づいて決定される。

【0008】また、この発明の第2の観点にかかる認証システムは、コンピュータが所定の処理に従って表示す

る、データの書き込みが可能なウィンドウへ、前記データを書き込むことを許すか否かを決定する認証システムであって、前記ウィンドウを識別するウィンドウ識別情報を記憶するウィンドウ識別情報記憶手段と、登録者の身体の特徴を表す身体情報と、前記ウィンドウに書き込むべきデータとを互いに対応付けて記憶する登録者情報記憶手段と、前記コンピュータが、前記ウィンドウ情報記憶手段に記憶されている前記ウィンドウ識別情報が示す前記ウィンドウを表示する処理を実行していることを検出し、検出された前記ウィンドウへのデータの書き込みを阻止するウィンドウ検出手段と、操作者の身体の特徴を表す情報を入力して、入力された前記情報と、前記登録者情報記憶手段に記憶されている前記身体情報とが実質的に一致するか否かを判別する身体情報認証手段と、一致すると判別された場合に、一致すると判別された前記身体情報に対応付けられている前記データを、前記ウィンドウ検出手段により検出された前記ウィンドウに書き込むデータ書込手段とを備える、ことを特徴とする。

【0009】このような認証システムによれば、前記ウィンドウ検出手段により検出された前記ウィンドウへの前記操作者によるデータの書き込みが阻止される。そして、前記操作者がそのウィンドウに書き込むべき前記データは、当該操作者が前記身体情報を提供した結果、その身体情報が前記登録者を示す前記身体情報と実質的に一致すると判別されたときに、前記データ書込手段によりそのウィンドウに書き込まれる。このため、当該ウィンドウが、特定の処理の実行の可否を決定するために所定のプログラムに従って開かれるウィンドウであれば、当該プログラムを変更することなく、その特定の処理の実行の可否が、前記操作者及び前記登録者の身体の特徴を表す情報に基づいて決定される。

【0010】前記コンピュータは、識別データの書き込みを要求する認証ウィンドウを表示し、当該認証ウィンドウに書き込まれたデータが前記識別データであると判別されたとき、所定の処理を実行する識別データ認証処理を実行するものであり、前記認証ウィンドウに書き込まれたデータが、前記識別データ認証処理に従って前記識別データであると判別されるために前記データが備えるべき条件を、実質的に無作為に変更する識別データ条件変更手段と、前記登録者情報記憶手段に記録されている、前記認証ウィンドウに書き込むべき前記データを、前記識別データ条件変更手段が変更した前記条件に合致するように変更するデータ書換手段とを備えるものであってもよい。

【0011】これにより、前記登録者が前記認証ウィンドウに書き込むべきデータは、当該登録者が関知しない内容を有するように変更される。このため、当該登録者の身体の特徴を表す情報が入力されることなく、前記所定の処理が実行されることが防止される。なお、前記条

件は任意であり、例えば、「前記データが特定の文字列であること」を以て前記条件としてもよいし、また、前記データが数値である場合、例えば、「前記データの値を特定の数で除した剰余が特定の値であること」を以て前記条件としてもよい。

【0012】前記登録者情報記憶手段は、複数の前記登録者を示す前記身体情報と、前記登録者の各々がデータを書き込むことを許される前記ウィンドウを示す前記ウィンドウ識別情報と、そのウィンドウに書き込むべきデータとを、互いに対応付けて記憶する手段を備え、前記データ書込手段は、前記身体情報認証手段の判別結果と、前記登録者情報記憶手段に記憶されている情報とに基づき、前記ウィンドウ検出手段により検出された前記ウィンドウが、前記操作者が前記データを書き込むことを許されているウィンドウであるか否かを判別し、書き込むことを許されているウィンドウであると判別されたとき、前記操作者が当該ウィンドウに書き込むべきデータを当該ウィンドウに書き込む手段を備えるものであってもよい。これにより、前記登録者が前記データを書き込むべき対象のウィンドウは、登録者毎に個別に指定される。

【0013】前記ウィンドウ識別情報記憶手段は、前記ウィンドウに書き込むべき前記データの種類の示す情報を、前記ウィンドウ識別情報と対応付けて記憶する手段を備え、前記データ書込手段は、前記ウィンドウ検出手段により検出された前記ウィンドウに、前記操作者が当該ウィンドウに書き込むべき前記データのうち、当該ウィンドウに書き込むべき前記データの種類の合致すると判別されるデータを書き込む手段を備えるものであってもよい。これにより、前記特定のウィンドウに書き込むべき前記データの種類の、前記特定のウィンドウ毎に個別に指定される。

【0014】前記ウィンドウ識別情報記憶手段は、前記ウィンドウ上にある前記データの書き込み箇所を示す情報と、当該書き込み箇所に書き込むべき前記データの種類の示す情報とを、前記ウィンドウ識別情報と対応付けて記憶する手段を備え、前記データ書込手段は、前記ウィンドウ検出手段により検出された前記ウィンドウ上にある前記データの書き込み箇所に、前記操作者が当該ウィンドウに書き込むべき前記データのうち、当該書き込み箇所に書き込むべき前記データの種類の合致すると判別されるデータを書き込む手段を備えるものであってもよい。これにより、前記ウィンドウに書き込むべき前記データの種類の、前記ウィンドウ上にある前記書き込み箇所毎に個別に設定される。

【0015】前記ウィンドウ識別情報記憶手段及び前記登録者情報記憶手段の少なくとも一方に格納されている情報は暗号化されており、前記ウィンドウ検出手段及び前記データ書込手段の少なくとも一方は、前記ウィンドウ識別情報記憶手段及び前記登録者情報記憶手段の少な

くとも一方に格納されている暗号化された情報を復号化する手段を備えるものであってもよい。これにより、前記ウィンドウ識別情報、身体情報、前記登録者が前記ウィンドウに書き込むべきデータ、前記ウィンドウに書き込むべきデータの種類の示す情報の少なくともいずれかは、外部からの不正なアクセスを受けても暗号化されたままの状態を取得されるにとどまるので、これらの情報の内容が漏洩することが防止される。

【0016】現在時刻を示す情報を前記身体情報認証手段に供給するタイマを備え、前記身体情報認証手段は、自らが行った前記判別の結果を示す情報及び該判別を行った時刻を示す情報を互いに対応付けて記憶するログ記録手段を備えるものとすれば、前記認証システムへの外部からの不正なアクセスの履歴の情報が取得される。

【0017】前記データ書込手段は、前記操作者の身体の特徴を表す情報が、前記登録者の身体の特徴を表す前記身体情報と一致しないと判別されたとき、前記ウィンドウ検出手段が検出した前記ウィンドウを消去する手段を備えるものとすれば、前記ウィンドウに、不正な手法によるデータの書き込みが行われることが防止される。

【0018】前記ウィンドウ検出手段は、前記ウィンドウ識別情報が示す前記ウィンドウが表示されたか否かを所定の時間間隔で検出する手段を備えることにより前記ウィンドウを検出してもよいし、また、前記ウィンドウ検出手段は、前記ウィンドウを書き込み可能な状態で表示することを前記コンピュータに要求する命令を取得することにより、前記コンピュータが当該ウィンドウを書き込み可能な状態で表示することを検出する手段を備えることによつて、前記ウィンドウを検出してもよい。

【0019】前記登録者の身体の特徴を表す前記身体情報は、例えば、該登録者の指の特徴を示す情報からなり、その場合、前記身体情報認証手段は、前記操作者の指の特徴を示す情報を読み取る手段を備えるものであってもよい。

【0020】前記ウィンドウ検出手段は、検出した前記ウィンドウの少なくとも一部を隠蔽する手段を備えることにより、自らが出した前記ウィンドウへの、操作者による前記データの書き込みを阻止するものであってもよい。

【0021】また、この発明の第3の観点にかかる認証システムは、データを入力するデータ入力処理を実行するシステムへの前記データの入力の可否を決定する認証システムであつて、前記システムが、所定の条件に合致する前記データ入力処理を実行していることを検出したとき、前記操作者による前記システムへの前記データの入力を阻止するデータ入力処理検出手段と、前記データ入力処理検出手段により検出されるべき前記データ入力処理を実行中の前記システムへの前記データの入力を許される者を識別する識別情報を記憶する識別情報記憶手段と、前記操作者を特定する情報を外部より入力し、そ

の情報と、前記識別情報とに基づき、前記操作者が、前記データ入力処理検出手段により前記データの書き込みを阻止された前記システムへの当該データの入力を許されている者であるか否かを判別し、許されていると判別されたとき、当該システムに当該データを入力するデータ入力手段とを備える、ことを特徴とする。

【0022】このような認証システムによれば、前記所定の条件に合致すると判別された前記データ入力処理を実行している前記システムへの前記操作者による前記データの入力が阻止される。そして、前記操作者が当該データ入力処理を実行している前記システムに前記データを入力することが許される者であると判別されたときには、前記データ入力手段により、そのシステムに前記データが書き込まれる。このため、前記データ入力処理が、特定の処理の実行の可否を決定するために、当該特定の処理を制御するプログラムの制御に従って実行されるものであれば、当該プログラムを変更することなく、その特定の処理の実行の可否が、前記操作者を特定する情報に基づいて決定される。

【0023】また、この発明の第4の観点にかかる、コンピュータ読み取り可能な記録媒体は、プログラムを実行する制御部と、前記制御部が供給する命令にตอบสนองしてデータの書き込みが可能なウィンドウを表示する表示部とを備えるプログラム実行手段を備えるコンピュータを、前記ウィンドウを識別するウィンドウ識別情報を記憶するウィンドウ識別情報記憶手段と、登録者の身体の特徴を表す身体情報と、前記ウィンドウに書き込むべきデータとを互いに対応付けて記憶する登録者情報記憶手段と、前記プログラム実行手段が、前記ウィンドウ識別情報記憶手段に記憶されている前記ウィンドウ識別情報が示す前記ウィンドウを表示する処理を実行していることを検出し、検出された前記ウィンドウへのデータの書き込みを阻止するウィンドウ検出手段と、操作者の身体の特徴を表す情報を入力して、入力された前記情報と、前記登録者情報記憶手段に記憶されている前記身体情報とが実質的に一致するか否かを判別する身体情報認証手段と、一致すると判別された場合に、一致すると判別された前記身体情報に対応付けられている前記データを、前記ウィンドウ検出手段により検出された前記ウィンドウに書き込むデータ書込手段と、して機能させるためのプログラムを記録したことを特徴とする。

【0024】このような記録媒体に記録されたプログラムを実行する前記コンピュータは、前記ウィンドウ検出手段により検出された前記ウィンドウへの前記操作者によるデータの書き込みが阻止され、前記操作者がそのウィンドウに書き込むべき前記データが、当該操作者が前記身体情報を提供した結果、その身体情報が前記登録者を示す前記身体情報と実質的に一致すると判別されたときに、前記データ書込手段によりそのウィンドウに書き込まれる認証システムとして機能する。このため、当該

ウィンドウが、特定の処理の実行の可否を決定するために前記プログラムに従って開かれるウィンドウであれば、当該プログラムを変更することなく、その特定の処理の実行の可否が、前記操作者及び前記登録者の身体の特徴を表す情報に基づいて決定される。

【0025】

【発明の実施の形態】以下、この発明の実施の形態にかかる認証システムを、操作者の指紋を判別して特定のコンピュータプログラムの利用を許可するか否かを決定する指紋認証システムを例として説明する。

【0026】図1は、この指紋認証システムの物理的構成を示す。図示するように、この指紋認証システムは、指紋読取部1と、入力部2と、表示部3と、主記憶部4と、外部記憶部5と、制御部6とより構成される。

【0027】指紋読取部1は、人間の指の輪郭の画像を読み取って、その画像データを制御部6へ供給するための装置であり、制御部6から指紋読み取りの許可を受けたときに、指の輪郭の画像を読み取る。入力部2は、ユーザが文字等のデータ等を入力するための入力装置であり、キーボード、マウス等を備える。入力部2は、ユーザの操作に従った情報を制御部6へ供給する。表示部3は、陰極線管(CRT)、液晶ディスプレイ(LCD)等からなり、制御部6の指示に従って、画像を表示する。

【0028】主記憶部4は、RAM(Random Access Memory)等からなり、制御部6の作業領域として用いられる。

【0029】外部記憶部5は、ハードディスク装置等からなり、後述するウィンドウシステム51、監視プログラム52、データ送信プログラム54、設定登録プログラム55及び指紋認証プログラム53のそれぞれのプログラムコードと、ウィンドウリスト61、コントロールリスト62及び登録者リスト63を記憶する。そして、制御部6の指示に従い、記憶している情報を制御部6に出力する。

【0030】制御部6は、CPU(Central Processing Unit)等により構成され、ウィンドウシステム51、監視プログラム52、データ送信プログラム54、設定登録プログラム55及び指紋認証プログラム53を読み込み、後述の通りに実行する。

【0031】また、図2に示すように、この指紋認証システムは、論理的には、ウィンドウシステム51と、監視プログラム52と、データ送信プログラム54と、設定登録プログラム55と、指紋認証プログラム53と、ウィンドウリスト61と、コントロールリスト62と、登録者リスト63とより構成される。

【0032】ウィンドウシステム51は、制御部6により実行されるオペレーティングシステムであり、例えば、マイクロソフト社のウィンドウズ(商標)等からなる。ウィンドウシステム51は、ウィンドウシステム5

1 が呼び出す関数として制御部 6 により実行されるアプリケーション（例えば、監視プログラム 5 2、データ送信プログラム 5 4、設定登録プログラム 5 5 及び指紋認証プログラム 5 3）の処理を制御する。また、ウィンドウシステム 5 1 は、各アプリケーションにより呼び出されることにより、後述する所定の処理を実行する関数を備えている。

【0033】監視プログラム 5 2 は、ウィンドウシステム 5 1 の処理が開始されると、ウィンドウシステム 5 1 により自動的に呼び出されるアプリケーションであり、外部記憶部 5 に予め格納される。監視プログラム 5 2 の制御の下にある制御部 6 は、後述する処理を実行することにより、ウィンドウシステム 5 1 上で動作するアプリケーションにより表示画面の最前面に表示されるウィンドウ（すなわち、そのウィンドウと表示領域が重なる全てのウィンドウが、そのウィンドウにより隠されるように表示されるウィンドウ）を特定する。そして、特定されたウィンドウが、操作者に関するデータを書き込むべき監視対象ウィンドウ（すなわち、データ送信プログラム 5 4 の処理によるデータの入力が行われる対象のウィンドウ）であるか否かを後述する処理に従って判断する。

【0034】データ送信プログラム 5 4 は、監視プログラム 5 2 により呼び出されるアプリケーションであり、外部記憶部 5 に予め格納される。データ送信プログラム 5 4 の制御の下にある制御部 6 は、監視プログラム 5 2 により特定された監視対象ウィンドウに、指紋認証プログラム 5 3 により特定された登録者に関するデータのうち、登録者リスト 6 3 に格納されているデータを書き込む。

【0035】設定登録プログラム 5 5 は、操作者等の指示により起動されるアプリケーションであり、外部記憶部 5 に予め格納される。設定登録プログラム 5 5 の制御の下にある制御部 6 は、監視プログラム 5 2 により監視されるべきウィンドウを示す情報と、当該ウィンドウに書き込むべきデータの種類の示す情報とを、操作者の指示等に従って、ウィンドウリスト 6 1 に新たに登録する。また、設定登録プログラム 5 5 の制御の下にある制御部 6 は、登録者に関する後述の各種のデータを、操作者の指示等に従って、登録者リスト 6 3 に新たに登録する。

【0036】指紋認証プログラム 5 3 は、監視プログラム 5 2 により呼び出されるアプリケーションであり、外部記憶部 5 に予め格納される。指紋認証プログラム 5 3 の制御の下にある制御部 6 は、指紋読取部 1 が読み取った指紋の画像データに基づき、操作者が登録者であるか否かを判断し、認証結果を示す情報を監視プログラム 5 2 に引き渡す。

【0037】ウィンドウリスト 6 1 は、監視プログラム 5 2 により監視される対象のウィンドウに関する情報を

格納するデータベースであり、システム管理者等により予め外部記憶部 5 に格納され、また設定登録プログラム 5 5 により更新される。

【0038】ウィンドウリスト 6 1 は、図 3 に示すデータ構造を有する。図示するように、ウィンドウリスト 6 1 は複数のレコードからなり、各レコードの先頭の記憶領域には、設定登録プログラム 5 5 が後述する処理において各々の監視対象ウィンドウに固有に割り当てた識別番号が格納されている。続く記憶領域には、各々の監視対象ウィンドウを表示させるアプリケーションが指定する文字列であり、当該ウィンドウの種別を表すものである「ウィンドウクラス」が格納されている。続く記憶領域には、監視対象ウィンドウが表示されたとき、その表題として当該ウィンドウ上の所定の位置に表示される文字列である「ウィンドウテキスト」が格納されている。

【0039】続く記憶領域には、データを書き込むために各監視対象ウィンドウ上に表示されるウィンドウ（以下、「コントロール」と呼ぶ）のうち、登録者を識別するために各登録者に固有の識別符号（個人 ID）を書き込むべきコントロールを特定する識別情報が格納されている。そして、更に続く記憶領域には、パスワードを書き込む対象のコントロールを特定する識別情報が格納されている。

【0040】コントロールを特定する識別情報には、例えば、コントロールに、監視対象ウィンドウと同様に割り当てられている、ウィンドウクラス及び／又はウィンドウテキストが含まれ、また、各々のコントロールが表示される対象の監視対象ウィンドウ上での、そのコントロールの位置を示す情報が含まれる。

【0041】なお、コントロールには、例えば、各監視対象ウィンドウに含まれる記入欄（エディット）、チェックの有無を表示するチェックボックス、ボタンスイッチのオン又はオフの状態を図示するプッシュボタン等が含まれる。

【0042】コントロールリスト 6 2 は、各コントロールのうち、個人 ID を書き込むべきもの及びパスワードを書き込むべきものを除いたコントロールに関する情報を格納するデータベースである。コントロールリスト 6 2 は、図 4 に示すデータ構造を有する。図示するように、コントロールリスト 6 2 は複数のレコードからなり、各レコードの先頭の記憶領域には、各々のコントロールが属する監視対象ウィンドウの識別番号が格納されている。次の記憶領域には、当該コントロールを特定するための識別情報が格納され、続く記憶領域には、そのコントロールの種別（例えば、エディットや、チェックボックス、プッシュボタン等）を示す情報が格納される。続く記憶領域には、そのコントロールについて行う操作（例えば、「チェックボックスをオンにする」「プッシュボタンを押す」等の操作）を示す情報が格納される。そして、当該操作が「文字列を送信する」操作を示



すものである場合、続く記憶領域には、送信すべき文字列が、後述する登録者リスト63に格納されている、第1～第3の3種類の送信データのうち、いずれの種類のデータであるかを示す情報が格納されている。

【0043】登録者リスト63は、監視対象ウィンドウに書き込むべきデータを格納するリストであり、システム管理者等により予め外部記憶部5に格納され、設定登録プログラム55により更新される。

【0044】登録者リスト63は、図5に示すデータ構造を有する。図示するように、登録者リスト63は、複数のレコードからなり、各レコードの先頭には、登録者の氏名が格納される。各レコードの、氏名に続く記憶領域には、その氏名を有する登録者の個人IDと、パスワードが格納されている。

【0045】パスワードに続く記憶領域には、各登録者の指の輪郭の特徴を表す特徴データが格納されている。特徴データは、例えば、以下の手順により得られたものである。まず、予め指紋読取部1と実質的に同一の指紋読取器により読み取られた、図6(a)に示すような登録者の指の画像の輪郭線を、図6(b)に示すように適当な間隔で分割し、横方向に対応した輪郭線の高さの配列 $[h_1, h_2, \dots, h_7]$ を得る。そして、同一の指を読み取って得られた複数個の画像について同一の操作を行い、横方向に対応した輪郭線の高さの配列を複数個生成してから、 $h_1, h_2, \dots$ 及び $h_7$ の平均値 $S_1, S_2, \dots, S_7$ 及び分散 $v_1, v_2, \dots, v_7$ を計算する。得られた平均値 $S_1, S_2, \dots, S_7$ 及び分散 $v_1, v_2, \dots, v_7$ を特徴データとして用いる。

【0046】特徴データに続く記憶領域には、監視対象ウィンドウに書き込まれるために、予めシステム管理者等により定められ、又は設定登録プログラム55の処理において、操作者等により任意に定められた、第1～第3の3種類の送信データ（例えば、監視対象ウィンドウを閉じるためにクリックされるプッシュボタンを押す操作を示す情報）が格納されている。

【0047】（動作）次に、この指紋認証システムの動作を、図7～図10を参照して説明する。図7は、監視プログラム52の処理を表すフローチャートである。図8は、指紋認証プログラム53の処理を表すフローチャートである。図9は、データ送信プログラム54の処理を表すフローチャートである。図10は、設定登録プログラム55の処理を表すフローチャートである。

【0048】（監視プログラム52及び指紋認証プログラム53の処理）この指紋認証システムは、起動すると、まずウィンドウシステム51を実行し、ウィンドウシステム51は、監視プログラム52を呼び出す。呼び出された監視プログラム52は、まず、所定の時間（例えば、ほぼ100ミリ秒）が経過する毎にステップS102に処理を移す処理（タイマ処理）を行うため、ウィ

ンドウシステム51に当該タイマ処理を行う機能であるタイマプロシージャの登録を要求する（ステップS101）。そして、ウィンドウシステム51はタイマプロシージャを開始する。

【0049】タイマプロシージャが開始されると、開始後、ほぼ100ミリ秒が経過する毎に、ウィンドウシステム51は、監視プログラム52がステップS102の処理を行うことを許可する。許可を受けた監視プログラム52は、ステップS102において、表示部3の表示画面上、最前面に表示されているウィンドウを特定するウィンドウシステム51の関数を呼び出す。この関数は、例えばウィンドウシステム51がマイクロソフト社のウィンドウズ95（商標）である場合、GetForegroundWindow()等であってよい。呼び出されたウィンドウシステム51の関数は、戻り値として、該当するウィンドウにウィンドウシステム51が予め一意的に割り当てた符号（ハンドル）を供給する。

【0050】次に、監視プログラム52は、ウィンドウシステム51より供給されたハンドルに該当するウィンドウのウィンドウクラス、ウィンドウテキスト及び表示画面上での表示領域の座標を供給するウィンドウシステム51の関数を呼び出す。これにより、監視プログラム52は、ウィンドウシステム51より、該当するウィンドウのウィンドウクラス、ウィンドウテキスト及び表示画面上での表示領域の座標データの供給を受ける。次いで、監視プログラム52は、供給されたウィンドウクラス及び／又はウィンドウテキストのデータをキーとしてウィンドウリスト61を検索し、当該キーにより特定されるウィンドウが索出されたか否かを判別する（ステップS103）。

【0051】ステップS103において、該当するウィンドウが索出されなかった場合、監視プログラム52は、ステップS101に処理を戻す。索出された場合は、索出されたウィンドウの利用者を認証するために、指紋認証プログラム53を呼び出し、ステップS103でウィンドウシステム51から供給された、ウィンドウの表示領域の座標データを指紋認証プログラム53に引き渡す（ステップS104）。

【0052】指紋認証プログラム53は、呼び出されると、まず、引き渡された座標データが示す表示領域に、指の輪郭の照合を促すメッセージを含むウィンドウを表示する。そして、指紋読取部1に指紋の読み取りを指示し、指紋読取部1から指の輪郭を表す画像情報が供給されるのを待機する。これにより、現在最前面にある監視対象ウィンドウは、指の輪郭の照合を促すメッセージを含むウィンドウにより覆い隠された状態となる。指紋読取部1は、操作者が提示した指の輪郭を読み取って、その指の輪郭を表す画像情報を生成し、指紋認証プログラム53を実行している制御部6に供給する（ステップS201）。



【0053】指紋を表す画像情報が制御部6に供給されると、指紋認証プログラム53は、その画像情報に基づき、登録者リスト63に保存されている特徴データを得た手法と実質的に同一の手法により、横方向に対応した、指の輪郭線の高さの配列を得る（ステップS202）。すなわち、図6を参照して説明したように、読み取った指の輪郭を、特徴データを生成するために用いた指の画像を分割したときと実質的に同一の間隔で分割し、分割した位置の輪郭線の高さ $r_1$ 、 $r_2$ 、 $r_3$ ・・・、 $r_7$ を求める。

【0054】次に、指紋認証プログラム53は登録者リスト63にアクセスし、登録者リスト63に格納されているすべての特徴データを順次読み込む（ステップS203）。そして、ステップS202で求めた輪郭線の高さ $r_1$ 、 $r_2$ 、 $r_3$ ・・・、 $r_7$ と各特徴データとを比較し、読み込んだ高さ $r_1$ 、 $r_2$ 、 $r_3$ ・・・、 $r_7$ の全てが平均 $S$ ±分散 $v$ の範囲にある特徴データがあるかを判別する（ステップS204）。

【0055】判別の結果、読み込んだ高さの全てが平均 $S$ ±分散 $v$ の範囲にある特徴データがあると判別されると、指紋認証プログラム53は、操作者が、当該特徴データにあたる指紋を有する登録者であると判別する（ステップS205）。次に、指紋認証プログラム53は、登録者リスト63のうち当該特徴データを含んだレコードから、登録者の氏名の情報を読み出す。そして、監視プログラム52に、認証結果を示す情報として、認証の成功を表す情報及び読み出された氏名の情報を供給し（ステップS206）、監視プログラム52に処理を戻す（リターンする）。

【0056】一方、読み込んだ高さの全てが平均 $S$ ±分散 $v$ の範囲にある特徴データがないと判別されると、指紋認証プログラム53は、認証の失敗を表す情報を、認証結果の情報として監視プログラム52に供給し（ステップS207）、監視プログラム52に処理を戻す。

【0057】監視プログラム52は、指紋認証プログラム53から認証結果を示す情報の供給を受けると、その情報が、認証の成功又は失敗のいずれを表すものであるかを判別する（ステップS105）。そして、認証の失敗を表すと判別されると、監視プログラム52は、ステップS103で素出されたウィンドウ（すなわち、現在最前面にあるウィンドウ）を閉じるようウィンドウシステム51に指示する。ウィンドウシステム51が当該ウィンドウを閉じると（ステップS107）、監視プログラム52は、タイマプロシージャとして登録されているステップS102の処理を行うことをウィンドウシステム51が許可するのを待って、許可があると、ステップS102に処理を戻す。

【0058】一方、認証結果を示す情報が、認証の成功を表すと判別されると、監視プログラム52は、データ送信プログラム54を呼び出す。そして、データ送信プ

ログラム54に、登録者リスト63のうち、当該登録者の氏名が含まれるレコードを特定する情報と、現在最前面にあるウィンドウ（すなわち、ステップS103で特定されたウィンドウ）の識別番号と、ステップS102で取得した、当該ウィンドウのハンドルとを供給する

（ステップS106）。データ送信プログラム54の処理が終了し、監視プログラム52に処理が戻ると、監視プログラム52は、タイマプロシージャとして登録されているステップS102の処理を行うことをウィンドウシステム51が許可するのを待って、許可があると、ステップS102に処理を戻す。

【0059】（データ送信プログラム54の処理）データ送信プログラム54が呼び出されると、データ送信プログラム54はまず、監視プログラム52より供給された情報が示す、登録者リスト63のレコードから、入力された指紋が示す登録者の個人ID（個人識別符号）と、パスワードとを読み出す（ステップS301）。

【0060】次に、データ送信プログラム54は、ウィンドウリスト61のうち、現在最前面にあるウィンドウの識別番号を含むレコードを特定し、そのレコードから、個人ID及びパスワードを書き込むべき各コントロールのウィンドウクラス及び／又はウィンドウテキストを読み出す。（ステップS302）。

【0061】次に、データ送信プログラム54は、ハンドルを引数として供給することによりそのハンドルが示すウィンドウに含まれるコントロールのハンドルを通知するウィンドウシステム51の関数を呼び出す。このとき引数としては、監視プログラム52より供給された、現在最前面にあるウィンドウのハンドルを供給する（ステップS303）。なお、当該関数は、例えば、ウィンドウシステム51がウィンドウズ95である場合、GetWindow()でよい。呼び出された当該関数は、データ送信プログラム54より供給されたハンドルが示すウィンドウ（すなわち、現在最前面に表示されているウィンドウ）に含まれる各コントロールのハンドルを、戻り値としてデータ送信プログラム54に供給する。

【0062】データ送信プログラム54は、ウィンドウシステム51の関数より、現在最前面にあるウィンドウに含まれるコントロールのハンドルを取得すると、そのハンドルに該当するコントロールのウィンドウクラス及びウィンドウテキストを供給するウィンドウシステム51の関数を呼び出す（ステップS304）。これにより、データ送信プログラム54は、ウィンドウシステム51より、現在最前面にあるウィンドウに含まれるコントロールのウィンドウクラス及びウィンドウテキストの供給を受ける。

【0063】各コントロールのウィンドウクラス及びウィンドウテキストがウィンドウシステム51より供給されると、データ送信プログラム54は、これらのウィンドウクラス及びウィンドウテキストを、それぞれが示す

コントロールのハンドルと対応付けて、主記憶部4に格納する（ステップS305）。

【0064】次に、データ送信プログラム54は、ステップS305において主記憶部4に格納されたウィンドウクラス及びウィンドウテキストのうちから、ステップS302においてウィンドウリスト61より読み出したものと同一のウィンドウクラス及び／又はウィンドウテキストを特定する。そして、特定されたウィンドウクラス及び／又はウィンドウテキストに対応付けられているハンドルを読み出す（ステップS306）。これにより、個人IDを書き込むべきコントロールのハンドルと、パスワードを書き込むべきコントロールのハンドルとが特定される。

【0065】そして、データ送信プログラム54は、コントロールにデータを書き込むウィンドウシステム51の関数を呼び出し、ステップS306で特定された、個人IDを書き込む対象のコントロールのハンドルと、書き込むべき個人IDとを、この関数に供給する（ステップS307）。これにより、個人IDを書き込むべきコントロールに、登録者の個人IDが書き込まれる。なお、ステップS307で呼び出す関数は、ウィンドウシステム51が上述のウィンドウズ95である場合、例えば、SendMessage() でよい。

【0066】更に、データ送信プログラム54は、ステップS306で特定された、パスワードを書き込むべきコントロールに、ステップS307の処理と実質的に同一の処理により、パスワードを書き込む（ステップS308）。

【0067】次に、データ送信プログラム54は、監視プログラム52から供給された識別番号をキーとしてコントロールリスト62を検索し、当該識別番号を含むレコードを索出する（ステップS309）。そして、登録者リスト63のうち、ステップS301で個人IDとパスワードを読み込んだレコードから、第1の送信データを読み出す（ステップS310）。

【0068】次に、データ送信プログラム54は、ステップS309で索出された各レコードに格納されている、書込対象の送信データを指定する情報を検索することにより、索出された各コントロールのうちに、ステップS310又はS317で最後に読み込んだ送信データを書き込む対象のコントロールがあるか否かを判別する（ステップS311）。そして、書き込む対象のコントロールがないと判別されると、データ送信プログラムは処理をステップS316に移し、あると判別されると、処理をステップS312に移す。

【0069】ステップS312で、データ送信プログラム54は、ステップS311において送信データの書込対象として索出されたコントロールを示すレコードから、当該コントロールのウィンドウクラス及び／又はウィンドウテキストを読み出す。

【0070】そして、当該ウィンドウクラス及び／又はウィンドウテキストと実質的に同一のウィンドウクラス及び／又はウィンドウテキストを、ステップS305において主記憶部4に格納されたウィンドウクラス及びウィンドウテキストのうちから特定する。そして更に、特定されたウィンドウクラス及び／又はウィンドウテキストに対応付けられているハンドルを読み出す（ステップS313）。これにより、送信データの書き込み対象のコントロールのハンドルが特定される。

10 【0071】次に、データ送信プログラム54は、送信データの書込対象としてステップS311で索出されたコントロールを示すレコードから、コントロールの種別の情報を読み出して、該コントロールの種別を判別する（ステップS314）

【0072】コントロールの種別が判別されると、データ送信プログラム54は、引数として供給されたハンドルが示すコントロールに、当該コントロールの種別に適合した所定の手法によりデータを書き込むウィンドウシステム51の関数を呼び出す。そして、呼び出した関数の処理に従い、ステップS310又はS317で最後に読み込んだ送信データを、ステップS311で特定されたコントロールに書き込む（ステップS315）。

【0073】例えば、データ送信プログラム54は、ウィンドウシステム51がウィンドウズ95であって、第1の送信データを書き込むコントロールがエディットであると判別した場合、上述のSendMessage() を呼び出し、第1の送信データを、書き込み対象のコントロールのハンドルとともにSendMessage() に順次供給する。

【0074】次に、データ送信プログラム54は、ステップS301で読み込んだレコードに、次の送信データがあるか否かを判別する（ステップS316）。判別の結果、次の送信データがあると判別されると、データ送信プログラム54は、その送信データを読み込んで、処理をステップS311に戻す（ステップS317）。次の送信データがないとき、データ送信プログラム54は、監視プログラム52に処理を戻す。

【0075】（設定登録プログラムの処理）監視対象ウィンドウを新たに登録する場合、この指紋認証システムは、新たに登録する対象のウィンドウがウィンドウシステム51上でアクティブになっている（すなわち、現に表示されている）状態で、入力部2より、監視対象ウィンドウの登録の開始が指示されると、制御部6は、設定登録プログラム55を呼び出し、実行する。

【0076】処理が始まると、設定登録プログラム55は、ウィンドウシステム51より、表示対象として現在主記憶部4上に展開されている各ウィンドウに関する情報を取得する（ステップS401）。ステップS401において取得される情報には、各ウィンドウのウィンドウクラス、ウィンドウテキストが含まれ、また、各ウィンドウに含まれるコントロールについて、そのウィンド

ウクラス、ウィンドウテキスト、種別及びそのコントロールが含まれるウィンドウ上における位置を示す情報が含まれる。

【0077】次に、設定登録プログラム55は、取得した情報のうち、コントロール以外のウィンドウのウィンドウクラス及びウィンドウテキストの一覧リストを、登録対象のウィンドウの選択を促すメッセージとともに表示部3に表示させ、入力部2を用いてウィンドウが選択されるのを待機する(ステップS402)。ウィンドウの選択は、例えば、入力部2のマウスにより、一覧リストのうち選択対象のウィンドウの情報が表示されている部分をクリックするなどすることにより行われる。

【0078】そして、ウィンドウを選択する入力が入力部2を用いてなされると、設定登録プログラム55は、選択されたウィンドウのウィンドウクラス及びウィンドウテキストを示す情報を主記憶部4に格納する(ステップS403)。そして、その選択されたウィンドウの画像を表すビットマップを主記憶部4上に展開し、展開されたビットマップが表示画像を、選択されたウィンドウのダミー画像として表示部に表示させる(ステップS404)。

【0079】次に、設定登録プログラム55は、個人IDを書き込むべきコントロールの選択を促すメッセージを表示部3に表示させ、選択されたウィンドウに含まれるコントロールが、入力部2を用いて選択されるのを待機する(ステップS405)。コントロールの選択は、例えば、入力部2のマウスを用いて、ステップS404で表示されたダミー画像のうち、選択されたウィンドウに含まれるコントロールにあたる部分がクリックされることにより行われる。

【0080】そして、当該ダミー画像のうち、個人IDを書き込むべきコントロールにあたる部分がクリックされると、設定登録プログラム55は、クリックされた位置のダミー画像内における座標の値を、ウィンドウシステム51より取得する(ステップS406)。そして、ステップS401で取得された、各コントロールの位置を示す情報を検索することにより、選択されたウィンドウに含まれる各コントロールのうち、ステップS406で求められた座標を表示領域として含むものを特定する(ステップS407)。

【0081】次に、設定登録プログラム55は、ステップS401で取得された、各コントロールの種別を示す情報を検索することにより、ステップS407で特定されたコントロールがエディットであるか否かを判別し(ステップS408)、エディットでないと判別されると、処理をステップS405に戻す。一方、エディットであると判別されると、設定登録プログラム55は、そのエディットのウィンドウクラス及び/又はウィンドウテキストを主記憶部4と、当該コントロールの種別を示す情報(この場合は、エディットであることを示す情

報)を主記憶部4に格納する(ステップS409)。

【0082】次に、設定登録プログラム55は、パスワードを書き込むべきコントロールの選択を促すメッセージを表示部3に表示させ、選択されたウィンドウに含まれるコントロールが、入力部2を用いて選択されるのを待機する(ステップS410)。そして、パスワードを書き込むべきコントロールが、個人IDを書き込むべきコントロールと同様にして選択されると、設定登録プログラム55は、ステップS406、S407における処理と同様にして、選択されたコントロールを特定する(ステップS411)。次に、設定登録プログラム55は、ステップS409の処理と同様の処理を行うことにより、ステップS411で特定されたコントロールがエディットであるか否かを判別する(ステップS412)。そして、エディットであると判別されれば、そのコントロールのウィンドウクラス及び/又はウィンドウテキスト及び当該コントロールの種別を示す情報を主記憶部4に格納し(ステップS413)。エディットでないと判別されれば、処理をステップS410に戻す。

【0083】次に、設定登録プログラム55は、送信データを書き込むべき他のコントロールを選択するか、又は選択の終了を指示するよう促すメッセージと、選択の終了を指示するためのプッシュボタンを含むウィンドウを表示部3に表示させる。そして、入力部2を用いてコントロールの選択又は選択の終了の指示が行われるのを待機する(ステップS414)。コントロールの選択は、例えば、個人IDやパスワードを書き込むべきコントロールの選択と同様の手法により行われる。また、選択の終了の指示は、例えば、ステップS414において表示された、選択の終了を指示するためのプッシュボタンがクリックされることにより行われる。

【0084】入力部2を用いて、コントロールの選択又は選択の終了の指示が行われると、設定登録プログラム55は、コントロールの選択の終了が指示されたか、コントロールが選択されたかを判別する(ステップS415)。そして、選択の終了が指示されたと判別されると、設定登録プログラム55は、処理をステップS419に移す。コントロールが選択されたと判別されると、設定登録プログラム55は、選択されたコントロールを、ステップS406、S407における処理と同様の処理により特定する。そして、特定されたコントロールの種別を、ステップS401で取得された、各コントロールの種別を示す情報を検索することにより判別し、判別結果に基づいて、当該コントロールについて行うべき操作の内容を決定する(ステップS416)。すなわち、例えば当該コントロールがエディットであれば「文字列入力」、チェックボックスであれば「チェックのオン/オフ」を決定する。

【0085】次に、設定登録プログラム55は、特定されたコントロールに書き込むべきデータの種類の指定を

促すメッセージを表示部3に表示させる。そして、当該コントロールに書き込むべきデータの種別を指定する指示（例えば、第1～第3の送信データのうちのいずれを書き込むかを指定する指示や、プッシュボタンのオン又はオフの状態を指定する指示）が入力部2を用いてなされるのを待機する（ステップS417）。データの種別が指定されると、指定されたデータの種別を示す情報、特定されたコントロールのウィンドウクラス、ウィンドウテキスト、種別及び操作内容を示す情報とを主記憶部4に格納し（ステップS418）、処理をステップS414に戻す。

【0086】データを書き込むべきコントロールの選択が終了すると、ステップS419において、設定登録プログラム55は、選択されたウィンドウに割り当てたための、固有の識別番号を決定する。ただし、この識別番号は、ウィンドウリスト61に既に登録されている各ウィンドウの識別番号と重複しないよう決定される。

【0087】次に、設定登録プログラム55は、ウィンドウリスト61に新たなレコードを追加し、そのレコードの先頭にステップS419で決定された識別番号を書き込み、続いて、ステップS403で選択され、主記憶部4に格納されたウィンドウの情報を、ウィンドウクラス、ウィンドウテキストの順で書き込む（ステップS420）。

【0088】次に、設定登録プログラム55は、ステップS420で書き込みが行われたレコード内のデータ最後尾に続けて、個人IDを書き込む対象のコントロールの識別情報を書き込み、更に、パスワードを書き込む対象のコントロールの識別情報を書き込む（ステップS421）。

【0089】次に、設定登録プログラム55は、個人ID及びパスワード以外の送信データを書き込む対象のコントロールがある場合、そのうちの一つのコントロールを表すための新たなレコードをコントロールリスト62に追加する。そして、そのレコードに、該当するコントロールに関する情報を、そのコントロールの識別情報、種別、操作内容及び書き込むべき送信データの番号の順で書き込む（ステップS422）。

【0090】以下、設定登録プログラム55は、送信データを書き込むコントロールとして特定されたもののうち、ウィンドウリスト61に未だ登録されていない各コントロールの情報を、S422と実質的に同一の処理に従って、コントロールリスト62に順次追加する（ステップS423）。特定された全てのコントロールの情報がコントロールリスト62に追加されると、設定登録プログラム55は、処理を終了する。

【0091】以上説明した処理により、ウィンドウシステム51上で動作するアプリケーションの指示により監視対象ウィンドウが開いたとき、このウィンドウに重なるようにして指の画像の提示を要求するメッセージを含

むウィンドウが表示される。そして、提示された指の輪郭が、予め登録された登録者の指の輪郭と一致すると判別されると、その登録者の個人ID、パスワード及びその他当該監視対象ウィンドウに書き込むべきデータが自動的に書き込まれる。監視対象ウィンドウを開く指示を送ったアプリケーションは、書き込まれた個人ID及びパスワードに基づいて、例えば、後続の特定の処理を行うことを決定する。

【0092】なお、この指紋認証システムの構成は、上述のものに限られない。例えば、指紋認証プログラム53が操作者の認証に用いるパラメータは上述のものに限らず、例えば、指紋や、顔の特徴、網膜のパターン等、操作者及び登録者の任意の身体的特徴を表す任意のデータに基づいて認証を行ってよい。また、指紋認証プログラム53は、表示部3の表示画面の最前面に表示された監視対象ウィンドウを覆い隠す必要はなく、任意の手法により当該監視対象ウィンドウを書き込み不能な状態とすればよい。また、監視プログラム52が監視する対象のウィンドウは、個人IDやパスワードの入力を予定したコントロールを含むものである必要はない。

【0093】また、監視プログラム52は、操作者に指紋の提示を要求する毎に、その要求を行った日時や、認証が成功したか否かの別や、認証が成功した場合はその成功した認証の際に提示された指紋を有する登録者の個人ID等を、外部記憶部5に格納されたセキュリティログに追加するようにしてもよい。このセキュリティログは、この指紋認証システムのシステム管理者等が、不審者が認証を行おうとした形跡の有無をチェックするなどのために用いることができる。

【0094】また、監視プログラム52は、このセキュリティログ又は他のファイルに、失敗した認証の際に提示された指紋を表す画像データを記録してもよい。記録された画像データは、この指紋認証システムを不正に利用しようとする不審者の特定および当該不審者の行動の追跡などのために用いることができる。

【0095】また、ウィンドウリスト61、コントロールリスト62及び登録者リスト63に含まれるデータは暗号化されていてもよい。この場合、設定登録プログラム55は、ウィンドウリスト61、コントロールリスト62及び登録者リスト63に書き込むデータを暗号化してから書き込むようにすればよい。また、監視プログラム52及びデータ送信プログラム54は、ウィンドウリスト61、コントロールリスト62及び登録者リスト63に含まれるデータを復号化してから、ウィンドウリスト61、コントロールリスト62及び登録者リスト63を検索するようにすればよい。

【0096】また、登録者リスト63に登録されている各登録者に割り当てられるパスワードは、監視対象ウィンドウを表示させるアプリケーションが与える許可等に  
50 応じて、各登録者の意思によらずに変更されるようにし

てもよい。

【0097】これにより、例えば監視対象ウィンドウが何らかの原因により監視プログラム52による監視を受けなくなっても、登録者以外の者は、変更前のパスワードを知っているだけでは、監視対象ウィンドウに有効なパスワードを書き込むことができないようになる。また登録者も、自らに割り当てられたパスワードを知ることがないので、監視プログラム52、指紋認証プログラム53及びデータ送信プログラム54の処理によらなければ、アプリケーションが監視対象ウィンドウを表示させて行う個人認証を成功させることができなくなる。

【0098】パスワードの変更は、具体的には、例えば監視プログラム52が、図11に示すパスワード変更の処理（すなわち、以下説明するステップS501～S510の処理）を実行することにより行われる。

【0099】監視プログラム52は、この指紋認証システムが起動して、ウィンドウシステム51により呼び出されると、上述のステップS101の処理を行う前に、まず、登録者リスト63にアクセスして、各登録者の個人ID及びパスワードを読み出す（ステップS501）。次いで、監視プログラム52は、ウィンドウリスト61にアクセスして、監視対象ウィンドウのウィンドウクラス及びウィンドウテキストを読み出す（ステップS502）。

【0100】次に、監視プログラム52は、ウィンドウシステム51より、表示対象として現在主記憶部4上に展開されている各ウィンドウのウィンドウクラス及びウィンドウテキストと、それらのウィンドウを表示させているアプリケーションを示す情報とを取得する（ステップS503）。

【0101】そして、監視プログラム52は、ステップS503で読み込んだウィンドウクラス及びウィンドウテキストが示すウィンドウのうち、ステップS502で読み込んだウィンドウクラス及びウィンドウテキストが示すウィンドウと一致すると判別されるものを特定する（ステップS504）。すなわち、監視プログラム52は、現在表示されている監視対象ウィンドウを特定する。

【0102】次に、監視プログラム52は、ステップS503で取得した、各ウィンドウを表示させているアプリケーションを示す情報に基づいて、ステップS504で特定された監視対象ウィンドウを表示させているアプリケーションを特定する（ステップS505）。

【0103】次に、監視プログラム52は、ステップS505で特定されたアプリケーションの一つにデータを送信するウィンドウシステム51の関数を呼び出し、この関数に、パスワードの変更要求を示す情報と、当該アプリケーションが表示させた監視対象ウィンドウに登録者の一人が書き込むべき個人ID及びパスワードとを供

給する（ステップS506）。

【0104】ステップS506で供給されたパスワードの変更要求、個人ID及びパスワードを取得したアプリケーションは、例えばステップS506で監視プログラム52が呼び出した関数と実質的に同一の関数を呼び出すなどの手法により、監視プログラムに新たなパスワードを供給する。アプリケーションより新たなパスワードを取得した監視プログラム52は、登録者リスト63にアクセスし、登録者リスト63のうち、ステップS506でアプリケーションに供給した個人IDを含むレコードを索出する（ステップS507）。すなわち、監視プログラム52は、新たなパスワードの発行を受けた登録者に関する情報を含むレコードを、登録者リスト63より索出する。そして、監視プログラム52は、ステップS507で索出されたレコードに含まれているパスワードを、ステップS507で取得した新たなパスワードに書き換える（ステップS508）。

【0105】続いて、監視プログラム52は、ステップS506～S508でパスワードの変更を受けた登録者以外の登録者についても、ステップS506～S508と実質的に同一の処理により、パスワードの変更を行う（ステップS509）。

【0106】更に、監視プログラム52は、ステップS505で特定されたアプリケーションのうち、ステップS506～S509において新たなパスワードを発行したもの以外のものについても、ステップS506～S509と実質的に同一の処理を行って、各登録者のパスワードの変更を行う（ステップS510）。

【0107】以上説明したパスワード変更の処理により、起動中の各アプリケーションについて、各登録者のパスワードの変更が終了すると、監視プログラム52は、上述のステップS101以下の処理に移る。ステップS501～S510の処理により、各登録者のパスワードは各登録者の意思にかかわらず変更される。このため、パスワードの変更以後、各登録者は、例えば監視プログラム52の処理を何らかの手法により停止させても、パスワードが変更された監視対象ウィンドウに正しいパスワードを書き込むことができない。

【0108】なお、上述のパスワード変更の処理は、監視プログラム52が行う必要はなく、例えば別個のプログラムが当該処理を行ってもよいし、設定登録プログラム55が行ってもよいし、その他任意のプログラムが行ってもよい。また、上述のパスワード変更の処理は、アプリケーションが発する要求にตอบสนองして実行されてもよい。

【0109】また、監視プログラム52は、例えば、監視対象ウィンドウを表示させるアプリケーションが当該監視対象ウィンドウに書き込まれたデータを正しいパスワードとして認識する条件が既知であれば、そのアプリケーションに新たなパスワードの発行を要求する必要は

ない。この場合、監視プログラム52は、当該条件に合致する新たなパスワードを自ら生成して、登録者リスト63の、パスワード変更の対象である登録者を示すレコードに格納されているパスワードを、新たに生成したパスワードに更新すればよい。

【0110】また、各登録者に関する情報を書き込む対象の監視対象ウィンドウは、登録者毎に異なってもよい。この場合、例えば、登録者リスト63の各レコードに、各々の登録者に関するデータを書き込む対象の監視対象ウィンドウを特定する識別情報（例えば、当該監視対象ウィンドウのウィンドウクラス及び／又はウィンドウテキスト）が含まれていてもよい。

【0111】そして、登録者リスト63の各レコードが各々の登録者に関するデータを書き込む対象の監視対象ウィンドウを特定する識別情報を含んでいるとき、監視プログラム52は、更に、当該識別情報に基づいて、データの書き込みを行うか否かを判別してもよい。

【0112】具体的には、例えば、上述のステップS105の処理において、認証が成功したと判別されたとき、監視プログラム52は、登録者リスト63のうち、認証結果を示す情報と共に供給された登録者の氏名が格納されているレコードを特定する。そして、特定されたレコードに、現在最前面にあるウィンドウの識別情報が含まれているか否かを判別する。そして、判別の結果、現在最前面にあるウィンドウの識別情報が、当該レコードに含まれていないと判別されると、監視プログラム52はステップS107に処理を移し、含まれていると判別されると、ステップS106に処理を移す。

【0113】また、登録者リスト63の各レコードが、各々の登録者に関するデータを書き込む対象の監視対象ウィンドウを特定する識別情報を含むとき、設定登録プログラム55は、更に、登録者リスト63に当該識別情報を書き込むようにしてもよい。

【0114】具体的には、例えば、上述のステップS415の処理が終了した後、設定登録プログラム55は、登録者リスト63にアクセスし、登録者リスト63に含まれている各登録者の氏名の情報を読み出す。次に、設定登録プログラム55は、読み出した各登録者の氏名の一覧と、登録者の選択を促すメッセージと、選択終了を設定登録プログラム55に通知するためのプッシュボタンとを表示するウィンドウを表示部2に表示させ、入力部3を用いて登録者の選択がなされるのを待機する。

【0115】そして、例えば入力部3のマウスを用いて、当該ウィンドウ上の登録者の氏名を表示する箇所をクリックされた後、選択終了を通知するための上述のプッシュボタンをクリックされる等して登録者が選択されると、設定登録プログラム55は、登録者リスト63のうち、選択された登録者の氏名を含むレコードを特定する。次に、設定登録プログラム55は、特定されたレコードに、ステップS415までの処理により新たに監視

対象ウィンドウとして登録されたウィンドウのウィンドウクラス及び／又はウィンドウテキストを書き込み、処理を終了する。

【0116】なお、登録者リスト63の各レコードに、各レコードが示す登録者のデータを書き込む対象の監視対象ウィンドウの識別情報を書き込む処理は、設定登録プログラム55が行う必要はなく、例えば別個のプログラムが行ってもよい。またこの処理は、新たな監視対象ウィンドウが登録された直後にのみ行われる必要はない。例えば、設定登録プログラム55は、操作者の指示に従って、既に監視対象ウィンドウとして登録されているウィンドウの識別情報を、登録者リスト63のうち、当該識別情報が未だ格納されていないレコードに格納するようにしてもよい。

【0117】また、設定登録プログラム55は、既に登録者リスト63の各レコードに格納されている監視対象ウィンドウの識別情報を削除してもよい。また、ウィンドウリスト61の各レコードに含まれる、個人IDやパスワードを書き込む対象のコントロールの識別情報を編集するようにしてもよい。また、コントロールリスト62の各レコードに含まれる、送信データの種別を示す情報を編集するようにしてもよい。

【0118】また、設定登録プログラム55は、登録者が監視対象ウィンドウに書き込む対象のデータを登録する際、ダミーのウィンドウを表示する必要はない。例えば、設定登録プログラム55は、監視対象ウィンドウに含まれるコントロールのウィンドウクラス及び／又はウィンドウテキストを一覧表示してもよい。また、データを書き込むべきコントロールは、当該コントロールのウィンドウクラス及び／又はウィンドウテキストが、入力部2のキーボードを用いて操作者等により入力されることにより指定されてもよい。

【0119】また、設定登録プログラム55は、登録者が監視対象ウィンドウに書き込む対象のデータを登録する際、当該ウィンドウと形状が実質的に同一であり、ウィンドウ上にデータを表示するウィンドウシステム51の関数の処理に従ってデータを表示する、データ書き込み可能なダミーのウィンドウを表示してもよい。

【0120】この場合、設定登録プログラム55は、当該ダミーのウィンドウにデータを書き込む操作が行われることにより自らに供給されたデータを、ダミーのウィンドウに当該データを表示するウィンドウシステム51の関数に供給すると共に、登録者リスト63に書き込むようにしてもよい。

【0121】また、設定登録プログラム55は、監視対象ウィンドウに送信されるデータを、例えば監視対象ウィンドウへのデータの送信を行う関数をフックすることにより監視し、監視対象ウィンドウに送信されたデータを、監視対象ウィンドウに書き込むべきデータとして、登録者リスト63に書き込むようにしてもよい。

【0122】また、最前面に表示されているウィンドウを監視プログラム52が特定する手法は、上述のタイマを用いた手法に限られず、任意である。例えば、監視プログラム52は、アプリケーション等からウィンドウシステム51へ供給される、最前面に表示させるべきウィンドウを示す情報をフックする（すなわち、その情報が、ウィンドウシステム51以外のプログラムに従って実行される処理にも引き渡されるようにする）ことにより、最前面に表示されるウィンドウを特定してもよい。

【0123】具体的には、例えばウィンドウシステム51がウィンドウズ95である場合、監視プログラム52は、ウィンドウズ95により予め定められている形式の情報（メッセージ）である“WM\_ACTIVATE”が生成されるのを監視する。“WM\_ACTIVATE”は、オペレータの操作や、アプリケーションからのウィンドウ生成の要求などにより、特定のウィンドウを最前面に表示する必要が生じたときに、ウィンドウズ95のシステムにより生成され、最前面に表示されるべき当該ウィンドウを制御するプロシージャ（アプリケーション）に送信される。そして、監視プログラム52は、“WM\_ACTIVATE”と共に供給されている、最前面に表示すべきウィンドウのハンドルを取得すると、そのハンドルにより示されるウィンドウのウィンドウクラス及び／又はウィンドウテキストを、例えば、上述のステップS103における処理と同様にして取得する。すなわち、監視プログラム52は、ハンドルに該当するウィンドウのウィンドウクラス、ウィンドウテキスト及び表示画面上での表示領域の座標を供給するウィンドウズ95の関数を呼び出し、この関数から、当該ウィンドウのウィンドウクラス及び／又はウィンドウテキストを取得する。

【0124】以上、この発明の実施の形態を説明したが、この発明の認証システムは、専用のシステムによらず、通常のコンピュータシステムを用いて実現可能である。例えば、指紋読取部1に接続されたパーソナルコンピュータに上述の動作を実行するためのプログラムを格納した媒体（フロッピーディスク、CD-ROM等）から該プログラムをインストールすることにより、上述の処理を実行する認証システムを構成することができる。

【0125】また、コンピュータにプログラムを供給するための媒体は、通信媒体（通信回線、通信ネットワーク、通信システムのように、一時的且つ流動的にプログラムを保持する媒体）でも良い。例えば、通信ネットワークの掲示板（BBS）に該プログラムを掲示し、これをネットワークを介して配信してもよい。そして、このプログラムを起動し、ウィンドウシステムの制御下に、

他のアプリケーションと同様に実行することにより、上述の処理を実行することができる。

#### 【0126】

【発明の効果】以上説明したように、この発明によれば、既存のアプリケーションを変更することなく、特定の処理の実行の可否を登録者の身体情報に基づいて決定することができる認証システムが実現される。

#### 【図面の簡単な説明】

【図1】この発明の第1の実施の形態にかかる指紋認証システムの物理的構成を示すブロック図である。

【図2】この発明の第1の実施の形態にかかる指紋認証システムの論理的構成を示すブロック図である。

【図3】ウィンドウリストのデータ構造を示す図である。

【図4】コントロールリストのデータ構造を示す図である。

【図5】登録者リストのデータ構造を示す図である。

【図6】（a）は、指の輪郭の画像を表す図であり、（b）は、指の輪郭線の高さを表す図である。

【図7】監視プログラムの処理を示すフローチャートである。

【図8】指紋認証プログラムの処理を表すフローチャートである。

【図9】データ送信プログラムの処理を示すフローチャートである。

【図10】設定登録プログラムの処理を示すフローチャートである。

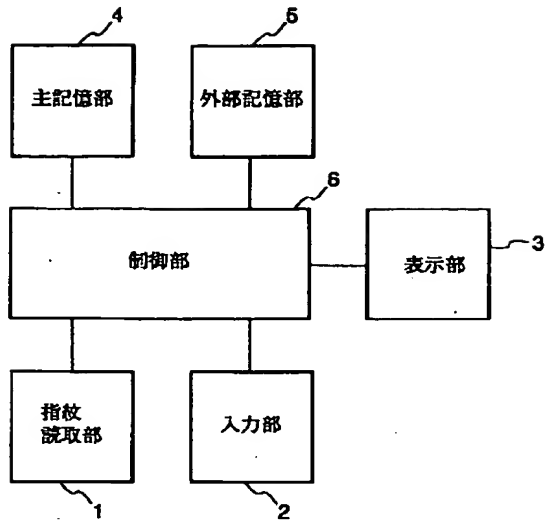
【図11】パスワード変更の処理を示すフローチャートである。

#### 【符号の説明】

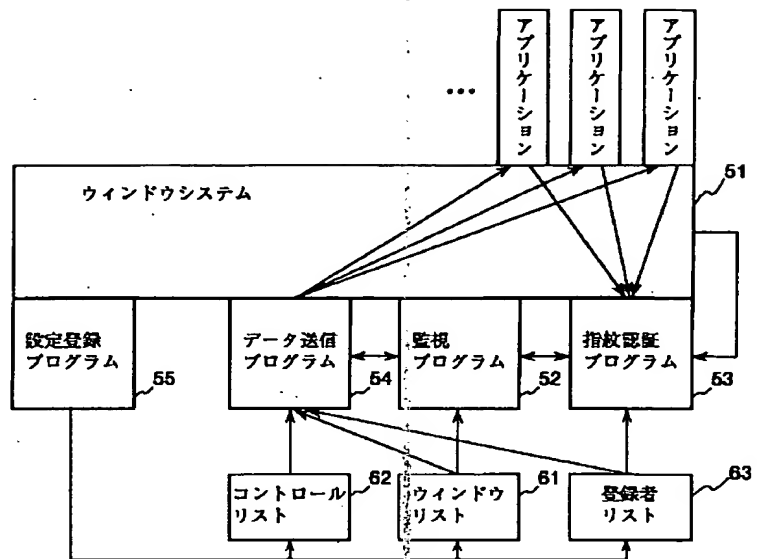
- |    |            |
|----|------------|
| 1  | 指紋読取部      |
| 2  | 入力部        |
| 3  | 表示部        |
| 4  | 主記憶部       |
| 5  | 外部記憶部      |
| 6  | 制御部        |
| 51 | ウィンドウシステム  |
| 52 | 監視プログラム    |
| 53 | 指紋認証プログラム  |
| 54 | データ送信プログラム |
| 55 | 設定登録プログラム  |
| 61 | ウィンドウリスト   |
| 62 | コントロールリスト  |
| 63 | 登録者リスト     |



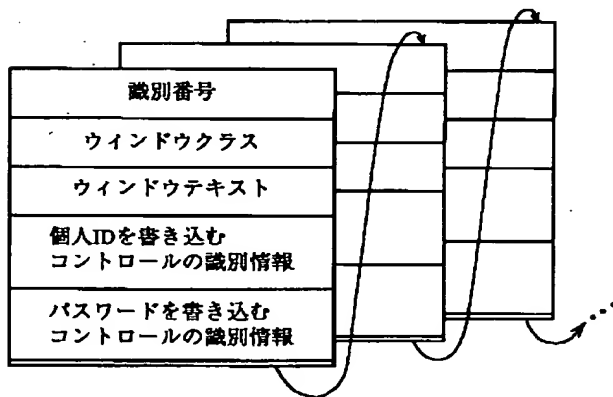
【図1】



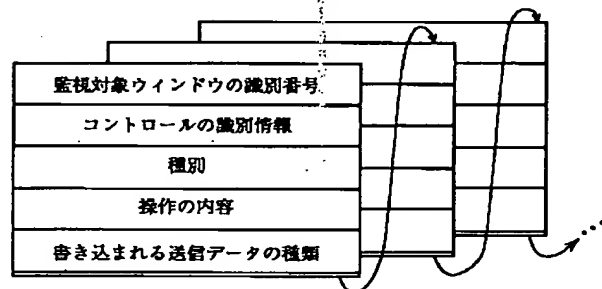
【図2】



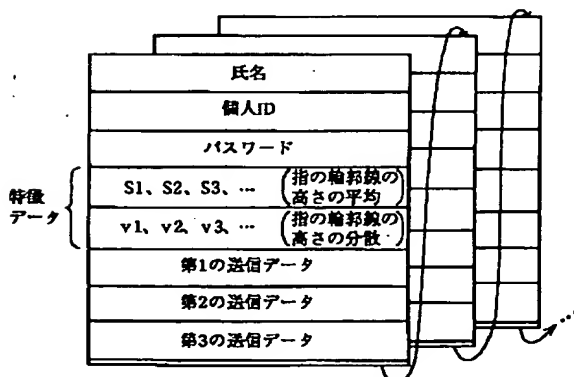
【図3】



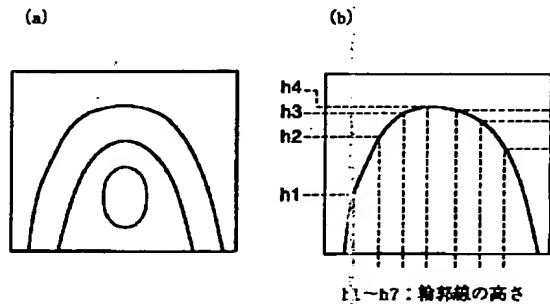
【図4】



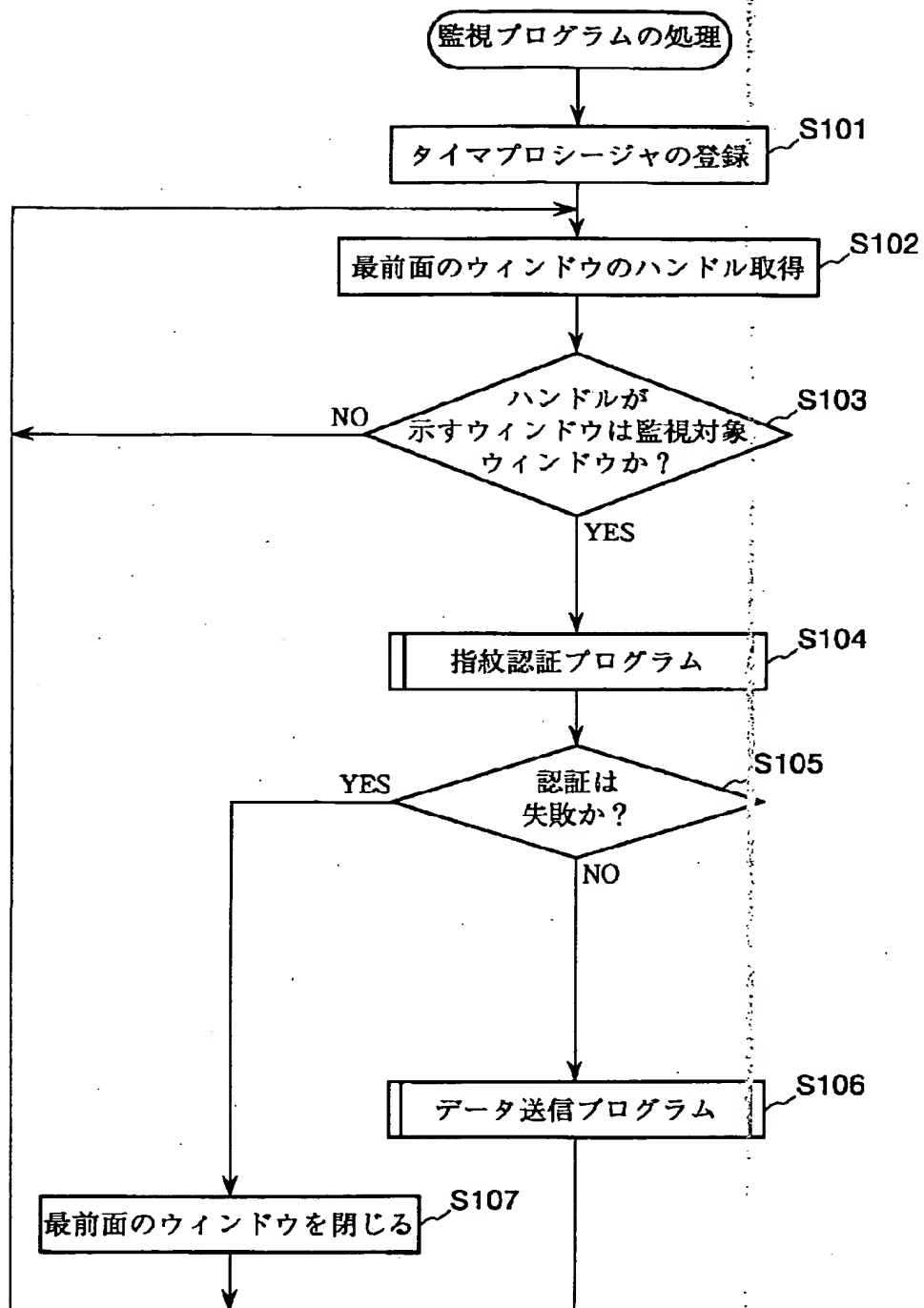
【図5】



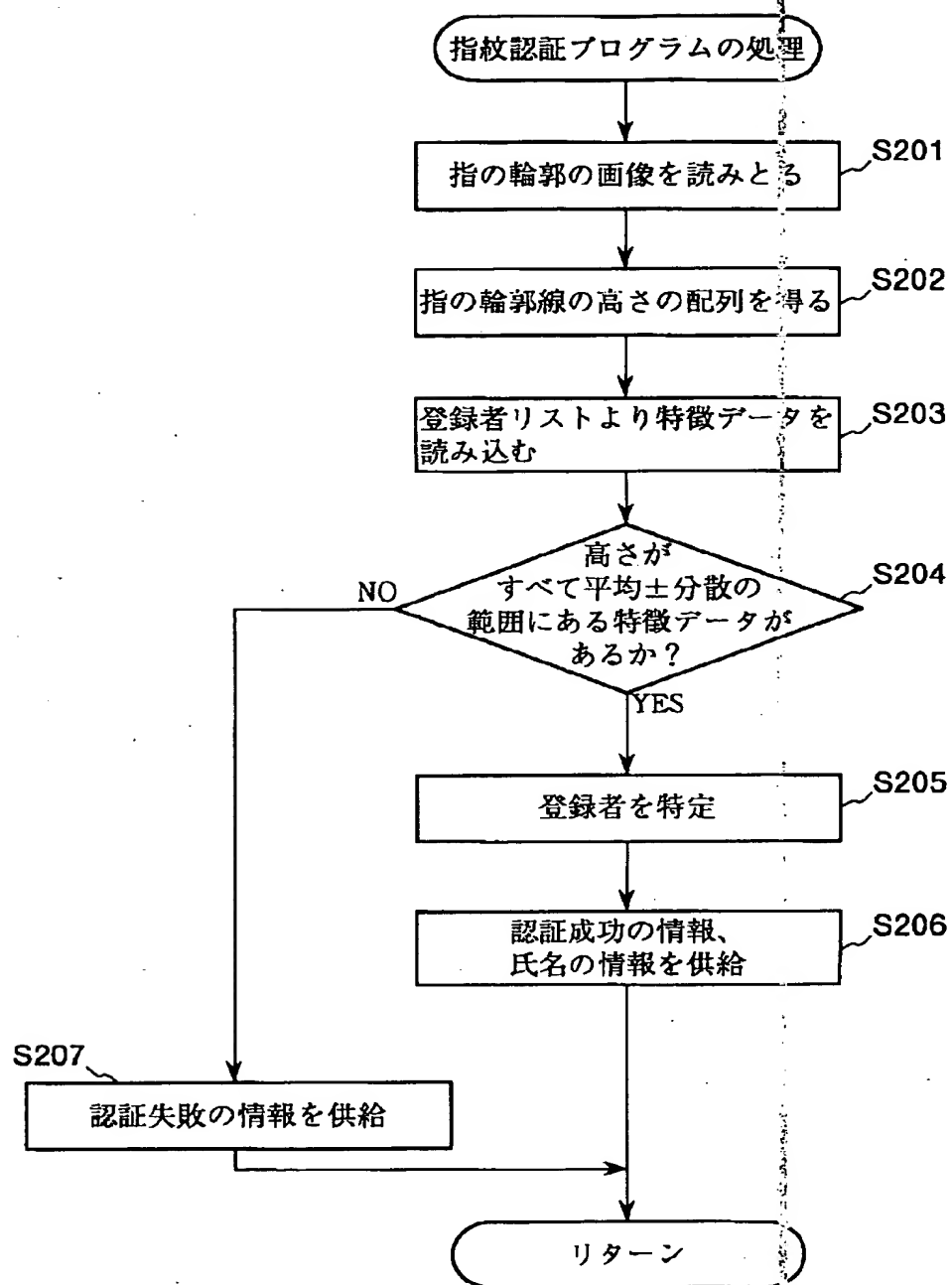
【図6】



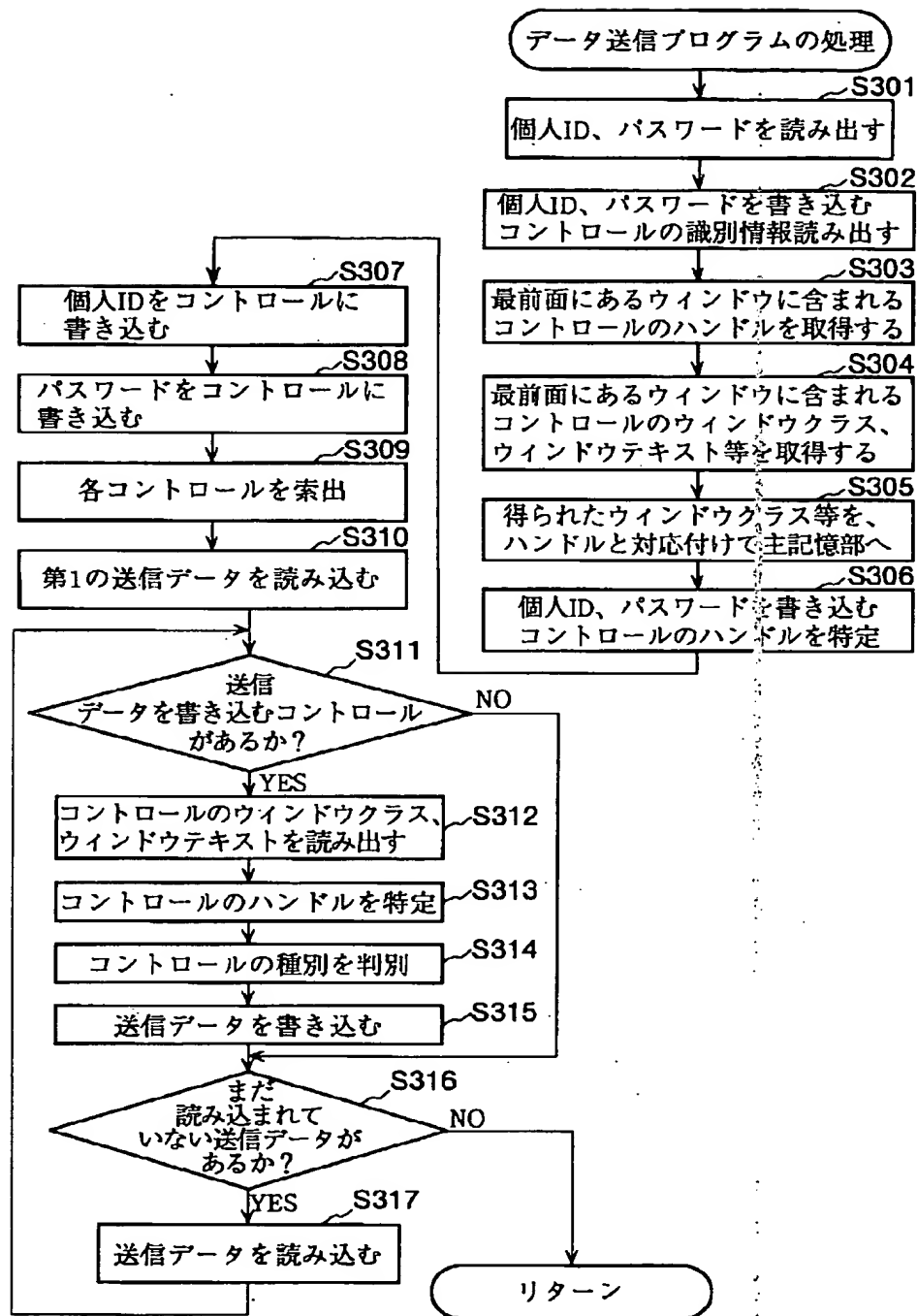
【図7】



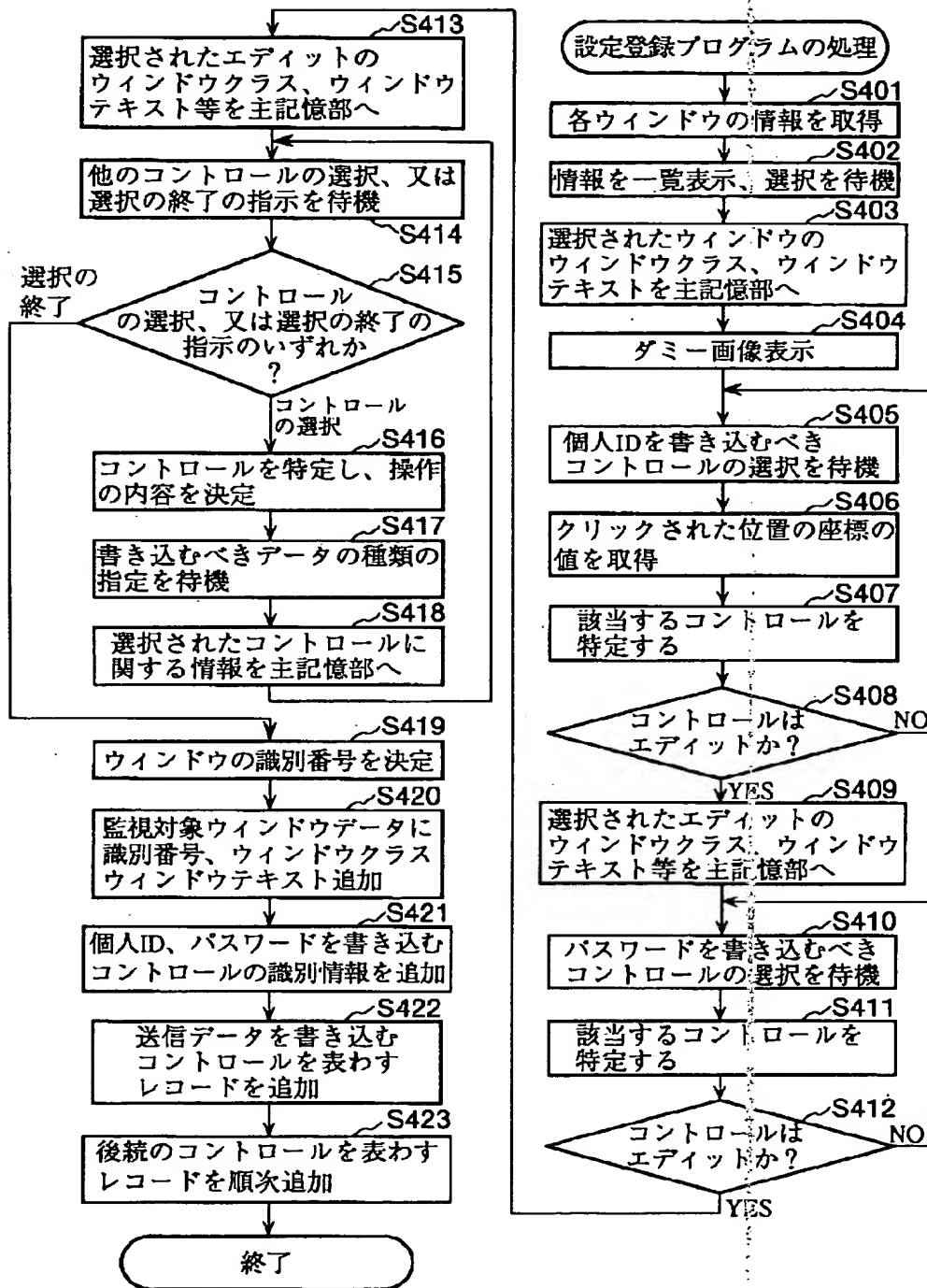
【図8】



【図9】



【図10】



【図11】

